IN THE UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF NEW YORK

BYTEMARK, INC.,	§	
	§	
Plaintiff,	§	
	§	
vs.	§	Civil Action No. 1:17-cv-01803
	§	
XEROX CORP., ACS TRANSPORT SOLUTIONS, INC., XEROX TRANSPORT SOLUTIONS, INC., CONDUENT INC., and NEW JERSEY TRANSIT CORP.,	§	
	§	
Defendants.	§	

MEMORANDUM IN SUPPORT OF MOTION TO COMPEL DOCUMENT PRODUCTION

Plaintiff Bytemark, Inc. files this Motion to Compel Defendants Xerox Corp., ACS Transport Solutions, Inc., Xerox Transport Solutions, Inc., Conduent Inc., and New Jersey Transit Corporation (collectively, "Defendants") to produce documents and information responsive to its First and Second Sets of Requests for Production (RFPs) (**Ex. A**, **Ex. B**), including request numbers 38-40 and 60-62. To date, Defendants have produced almost none of the information requested by Bytemark, aside from a smattering of publicly available documents, even though this information is clearly relevant to all of the claims in this case. For the reasons discussed herein, Bytemark requests that the Court grant this Motion.

I. BACKGROUND

Bytemark sued Defendants on March 3, 2017, alleging, *inter alia*, breach of contract, violation of the federal Defend Trade Secrets Act, misappropriation of trade secrets under New York Law and the New Jersey Trade Secret Act, unfair competition, and unjust enrichment. Dkt. #1, 74. Bytemark also has a pending motion before the Court to amend its complaint to add two patent infringement claims. Dkt. #104. Central to all of the allegations are Bytemark's visual validation mobile ticketing applications and systems (including, but not limited to, its V3 Ticketing Technology) and the accused New Jersey Transit app and MyTix app sold and offered for sale by Defendants, which Bytemark alleges incorporate its proprietary technology.

On December 27, 2018, Bytemark served its First Set of Requests for Production on Defendants ("First Set of RFPs"). *See* Ex. A (Bytemark's First Set of Requests for Production). In its Requests, Bytemark sought, e.g., information including documents regarding the creation and development of Defendants' accused systems. For example, Request No. 32 stated:

> **REQUEST NO. 32**: All documents showing the inception and development of any of Defendants' mobile ticketing application and/or system, including the MyTix application, including dates for each different design or model.

Id. at 9. In response to Bytemark's thirty-seven requests for production, Defendants responded with a collection of publicly available documents comprised mostly of annual reports and SEC filings. This production was nonresponsive to the vast majority of Bytemark's requests. Consequently, on February 14, 2019, Bytemark sent a letter advising Defendants of their failure to provide documents in response to its First Set of RFPs, including documents regarding the creation and development of the accused systems. *See* **Ex. C** (Bytemark Letter to Defendants, 2/14/2019).

On March 11, 2019, Defendants stated: **"we will make our confidential information available promptly after we've had a chance to review and understand Bytemark's alleged trade secret information."** *See* **Ex. D** (March 2019 Email Chain), at 6 (emphasis added). Defendants further stated that "[o]nce the protective order is entered, Defendants will produce limited, responsive discovery that Defendants can reasonably ascertain is relevant to this case," and "[o]nce Bytemark has reviewed the information produced by Defendants, the parties will meet and confer on any outstanding issues and Bytemark will serve a list of trade secrets it alleges Defendants have stolen." *Id.* at 4.

On December 23, 2019, the Court entered its protective order. Dkt. #102. Despite their earlier promise, Defendants did not, and have not, produced any additional discovery. Meanwhile, on February 3, 2020, Bytemark produced documents covered under the protective order to Defendants, and, the next day, Bytemark served its Second Set of Requests for Production ("Second Set of RFPs") requesting, *inter alia*, all versions of the accused New Jersey Transit app and MyTix app, the original API documentation for the MyTix app, and the mobile application source code for the first released version of the MyTix app. *See* Ex. B. For example, Request Nos. 38-40 state:

> **REQUEST NO. 38**: All documents and communications shared between Bytemark and Defendants using Privia project management software.
>
> **REQUEST NO. 39**: All documents and communications shared between Bytemark and Defendants using YouSendIt, Google Drive, Dropbox, and any filing sharing and/or cloud-based system.
>
> **REQUEST NO. 40**: All documents and communications shared between Bytemark and Defendants between 2012 and 2016.

Id. at 5-6. Request Nos. 60-62 state:

> **REQUEST NO. 60**: All versions of the New Jersey Transit app and MyTix app.
>
> **REQUEST NO. 61**: The original API documentation for the MyTix app.
>
> **REQUEST NO. 62**: The mobile application source code for the first released version of the MyTix app.

Id. at 8.

Once again, Defendants produced none of the requested documents and, instead, objected to all of Bytemark's requests. *See* **Ex. E** (Defendants' Objections and Responses to Plaintiff's Second Set of RFPs); **Ex. F** (June 2020 Email Chain). On June 2, 2020, Bytemark emailed Defendants about their refusal to produce any of these documents and met and conferred with them shortly thereafter. *See* Ex. F, at 4-7. **Bytemark informed Defendants that it would not be withholding any discoverable material, and Bytemark further agreed—pursuant to Defendants' request—to make available for inspection on or around August 14th *all* of its source code and confidential documents that include proprietary and trade secret-protected information.** *Id.* at 1-5. Bytemark extended this offer to Defendants several times. *Id.* Despite Bytemark's acquiescence to Defendants' request, Defendants continued to deny Bytemark access to the requested discovery. *Id.* On June 22, Defendants informed Bytemark that they were "withholding" their "highly confidential engineering information …. subject to [their] objections based on Bytemark's failure to identify its trade secrets and make them available for inspection."

Id. at 2-3. Defendants further stated that they were "preparing for production financial documents responsive to Bytemark's RFPs" and would produce "a majority of" "a set of documents from the Proposal Center that [Conduent] used with Bytemark." *Id.* at 2. However, Defendants have yet to produce this information, or *any* technical or non-publicly available information.

On August 11, 2020, Defendants expressly rejected Bytemark's offer to inspect its confidential and trade secrets information. *See* **Ex. G** (June/August 2020 Email Chain), at 1-3. Although Defendants have changed their position regarding discovery and Bytemark's purported obligation to specify its trade secrets with particularity as a prerequisite to receiving the requested information, Defendants' current position appears to be that they will not produce their source code or confidential information unless Bytemark agrees to provide a trade secrets misappropriation claim contention document that identifies with particularity each and every trade secret that Bytemark claims Defendants misappropriated. *See* Ex. G.

The parties filed a joint letter to the Court on December 10, 2020, requesting a hearing relating to discovery issues. On December 14, 2020, the Court denied the parties' request and ordered that any motions related to the parties' letter be filed by December 28, 2020. To date, Defendants have not produced documents responsive to Bytemark's forementioned discovery requests.

II. LEGAL STANDARD

Federal Rule 26 provides that "[p]arties may obtain discovery regarding any nonprivileged matter that is relevant to any party's claim or defense. Fed. R. Civ. 26(b)(1). "Although not unlimited, relevance, for purposes of discovery, is an extremely broad concept." *Bridges v. Corr. Servs.*, No. 17-CV-2220, 2020 WL 6899695, at *4 (S.D.N.Y. Nov. 24, 2020) (quoting *Condit v. Dunne*, 225 F.R.D. 100, 105 (S.D.N.Y. 2004)); *see also Oppenheimer Fund, Inc. v. Sanders*, 437

U.S. 340, 351 (1978) (noting that relevancy "has been construed broadly to encompass any matter that bears on, or that reasonably could lead to other matter that could bear on, any issue that is or may be in the case."). "Generally speaking, discovery is limited only when it is 'sought in bad faith, to harass or oppress the party subject to it, when it is irrelevant, or when the examination is on matters protected by a recognized privilege." *Trilegiant Corp. v. Sitel Corp.*, No. 09 Civ. 6492, 2011 WL 2693299, at *3 (S.D.N.Y. July 1, 2011) (quoting *In re Six Grand Jury Witnesses*, 979 F.2d 939, 943 (2d Cir. 1992)). "Once any possibility of relevance sufficient to warrant discovery is shown, the burden shifts to the party opposing discovery to show the discovery is improper." *Condit v. Dunne*, 225 F.R.D. 100, 106 (S.D.N.Y. 2004) (citations omitted); *In re Harcourt Brace Jovanovich, Inc. Sec. Litig.*, 838 F. Supp. 109, 114 (S.D.N.Y. 1993).

III. ARGUMENT

Defendants provide no tenable reason for their refusal to comply with Bytemark's requests for production. The source code and documents requested by Bytemark—which pertain to the accused systems at the center of this case—are clearly relevant to all of Bytemark's allegations, including breach of contract, misappropriation of trade secrets, unfair competition, and unjust enrichment. Indeed, this information is crucial for Bytemark to prove its case. Although Bytemark is aware of what confidential and proprietary information it has shared with Defendants, and although Bytemark believes that Defendants are using its technology and related system, Defendants alone have in their possession key information regarding the workings of their accused systems.

For example, Bytemark's breach of contract claim alleges that Defendants breached the parties' NDAs and Teaming Agreements "by using and/or disclosing Plaintiff's trade secrets and other confidential information to outside parties without Plaintiff's consent." Dkt. #74, ¶¶ 73-83.

Under these confidentiality agreements, the parties agreed, *inter alia*, "that any trade secrets or other confidential information shall remain the property of the originating party … and that the Xerox Entities had a duty to exercise all reasonable care to preserve and protect Plaintiff's trade secrets and other confidential information from unauthorized access, use, disclosure, or theft," that Defendants "[could] not reproduce Plaintiff's proprietary information in any form except as necessary to accomplish the NDA's intent," and that "[Bytemark's] inventions shall remain the property of the originating party … [and] disclosure and protection of proprietary information under the agreements shall be subject to the terms and conditions of the referenced NDAs." *Id.* ¶¶ 76-77. The information requested by Bytemark—e.g., "documents showing the inception and development of any of Defendants' mobile ticketing application and/or system, including the MyTix application," documents and communications shared between Defendants (including those using project management software), and API documentation and source code for the MyTix app—**is key evidence as to whether Defendants breached the confidentiality agreements and actually reproduced, used, disclosed and/or protected Bytemark's confidential and proprietary information**, whether through the accused MyTix application or any other mobile ticketing application and/or system.

Likewise, Bytemark's trade secrets misappropriation claims allege that Defendants have, e.g., "intentionally, willfully, and maliciously misused trade secrets and/or confidential or proprietary information or knowledge of Bytemark, and continue to do so, in breach of the Confidentiality Agreements and in violation of a confidential relationship and duty," have "misappropriated Plaintiff's trade secrets by using and/or disclosing them for their own economic benefit," and "misappropriated Plaintiff's confidential information and trade secrets by using and/or disclosing such confidential information and trade secrets by improper means for their own

personal gain." *Id.* ¶¶ 84-124. Again, the information requested by Bytemark **is vital evidence as to whether Defendants actually misused and/or disclosed Bytemark's confidential information and trade secrets for their own economic benefit or personal gain**.

Additionally, Bytemark's unfair competition claim alleges, e.g., that Defendants "misappropriated Plaintiff's labors and expenditures," "exploited Plaintiff's efforts and used its intellectual property and confidential information for Defendants' own commercial advantage," and "unlawful[ly] use[d] … Plaintiff's trade secrets in Defendants' applications that also have substantially the same look and feel." *Id.* ¶¶ 125-31. Bytemark's unjust enrichment claim alleges, e.g., that Defendants "have and continue to use and/or disclose Plaintiff's trade secrets and confidential information to develop and sell a competing mobile ticketing platform" and have therefore "benefitted by saving the significant time and cost that they would otherwise have had to incur to develop their own mobile ticketing platform." *Id.* ¶¶ 132-40. Once again, **the information requested by Bytemark, including Defendants' source code, documents relating to the inception and development of Defendants' accused systems, and communications shared between Defendants, is crucial to support these allegations**.

Thus, it is apparent that Bytemark's requests easily fall under Rule 26's "extremely broad" mandate, *see Bridges*, 2020 WL 6899695, at *4, and Defendants have not met their burden of showing that discovery is improper, *see In re Harcourt Brace Jovanovich*, 838 F. Supp. at 114; *Condit*, 225 F.R.D. at 106. Defendants' unilateral decision to withhold relevant information and their failure to produce *any* non-publicly available discovery to Bytemark is inappropriate and impermissible. Defendants' stonewalling is particularly egregious in light of (1) Bytemark's statement that it would not be withholding any discoverable material from Defendants and (2) Bytemark's concession to make available for inspection *all* of its source code and confidential

documents that include proprietary and trade secret-protected information prior to any production of confidential or proprietary materials by Defendants. *See* Ex. F. Defendants' demand that Bytemark specify with particularity what Defendants have stolen as a precondition to receiving *any* discovery relating to the development and technical aspects of Defendants' accused systems is unjustifiable and violates the Federal Rules, the Local Rules, and this Court's precedent.

No basis exists for Defendants' refusal to produce discoverable information that is central to this case (and which Defendants previously agreed to produce), and, accordingly, Bytemark asks that the Court compel Defendants to produce the requested documents and information.

IV. CONCLUSION

For the foregoing reasons, Bytemark respectfully requests that its motion to compel be granted in full.

Dated: December 28, 2020

Respectfully submitted,

s/ Dariush Keyhani
Dariush Keyhani
Keyhani LLC
1050 30th Street NW
Washington, DC 20007
Telephone: (202) 748-8950
Fax: (202) 318-8958
dkeyhani@keyhanillc.com
Attorneys for Plaintiff